THE A3C CONNECTION

Academic Computing and Communications Center April/May/June 2001

Email Filters and the Email Tools Page

Tech Tips

Any

CONTENTS

1 Email Filters via the ACCC Email Tools Page

3 Who Can Use Mailtools Email Filters?

5 Canned Spam Filters

6 How Mailtools Filters Work

8 SSH: Do You Know Where Your Password Is?

8 What is Safe? SSH, Bluestem, WebMail, Dialins

10 Secure X with SSH

Do you receive loads of lively email messages each day from **chess-l@nic.surfnet.nl** but you'd like to file them away in a special email folder to read when you get home from work? Perhaps you've had it with advertisements from **pet_turtles@example.com**, and you'd like all email from them to be automatically deleted. Or maybe you'd like everyone who sends you a message while you're at that conference next week to get an automatic reply telling them you'll get back to them when you return from your Caribbean cruise. (One can dream.)

Email filters can do all of this, and much more, and setting them up is now easy using the ACCC's Web Email Tools Utility, **http://www.uic.edu/htbin/accc/mailtools** There you will find links to several email tools, including two that you can use to create filters to automatically process your incoming email.

What Makes Mailtools Filters Different?

The filters you create using our Mailtools Web utility, which we'll call Mailtools filters, are different from the email filters that you create and use in Eudora or other local email clients, which we'll call local filters. There are two important and related differences: (1) Mailtools filters are only applied to *new incoming email*, whereas you can apply local filters to any email, new or old, incoming or outgoing; and (2) when Mailtools filters are used to sort messages into mailboxes, they can only put them into mailboxes *on the server*. Both of these differences are direct consequences of where the filters are kept:

Local filters reside on your personal computer; therefore local filters can't be applied to any incoming message until you download it (or at least its headers), that is, after you start your email program and it checks your mail for you. This is why a local email filter won't work to send automatic replies to the new incoming email you receive while you're away from the office — your local filter won't see any of your new mail until you come back and check your email. By then, it'll be too late.

Mailtools email filters, however, reside on an ACCC email server — icarus, mailserv, and tigger — and they act on *new incoming email* as soon as it arrives on the server, *before it even reaches your Inbox*. That makes them ideal for automatic vacation replies. But there's a drawback too. Because Mailtools filters live on the server, they can only sort incoming messages into email mailboxes that also live on the server. They can't sort messages into any local email mailboxes that you keep on your personal computer — you'll need a local email filter to do that. Nor can they do anything to outgoing email or to incoming email after it arrives in your Inbox or another mailbox on the server.

Whether this restriction of Mailtools email filters to move new incoming email only into mailboxes on the server will be a problem for you or not depends on how you read your email.

Two of the ACCC-supported email applications — WebMail and **pine** — are server-based; they always and only work with mailboxes that you keep on the server. Thus Mailtools' server-based filters are perfect for them.

Eudora and other local email applications can also manage email in mailboxes on the server, as long as you have configured them to use the IMAP protocol instead of the POP protocol to

System Icons:

The Internet and the World Wide Web

MS Windows

Apple Macintosh

Readership Icons:

Everyone

Novice

Expert

POP vs. IMAP

You can read more about the differences between IMAP and POP in the October/-November/December 1998 issue of the *A3C Connection*.

Also, the info in "Configuring Eudora for Windows for IMAP" should be all you'll need to convert any personal computer email program (including Outlook, Netscape, and Eudora for Macs) to use IMAP; it's at **http://www.uic.edu/depts/accc/software/eudora/eudora.win.imap.html**

manage your email. For our purposes, the important difference between IMAP and POP is that IMAP allows your email program to access all your email mailboxes, both the mailboxes that you keep locally on your personal computer and the mailboxes that you have on the server, while POP simply downloads all the mail from your Inbox in one shot and can only access local email mailboxes, the ones you have on your personal computer.

What email program you use and how you use it is only important if you choose ***File a message into a folder*** *as the* **action** *of a Mailtools filter.* Clearly in that case you would have to have access to the target mailbox. But Mailtools filters can do other things too. If you choose to use them to automatically forward or delete certain messages, for example, it certainly doesn't matter what email application you use or how you use it. That's the case for vacation autoreply filters — they simply generate a reply to incoming messages as they come in — and can be the case for the attachment and antispam filters too, if you set them up correctly.

How to Set Up Mailtools Filters

Getting Started: Email Tools Web Page

The Email Tools Web page is at:
http://www.uic.edu/htbin/accc/mailtools
Or you can go to the ACCC home page, **http://www.accc.uic.edu/**, click the **Email** button, then select **Email – Vacation Replies** or **Email Filters**.

Vacation Reply Messages

On the Email Tools page, select the ACCC server that your email account is on, select **Set up Email Vacation Reply** and click CONTINUE. Login using your ACCC netid and password, and you will be directed to a Web interface that allows you to easily set up an automatic reply to new incoming mail.

Step 1: Vacation Message

1. Type the message that you want to send in the box in Step 1, then click **Save Changes**.
2. When you receive Mailtools' reply, click **Return to the previous configuration page to verify the results.**, and make sure the message is correct.

Step 2: Activate or Deactivate the Vacation Program.

3. Click **activate vacation email**.
4. When you receive Mailtools' reply, click **Return to the previous configuration page to verify the results**.
5. Go on to Step 3 after you receive the confirmation email message in your Inbox.

Step 3: Set the date on which you want your vacation replies to end. You don't have to do this, but if you don't, you will have to remember to go back to Mailtools when you get back to turn your vacation autoreply off.

6. Select the MONTH, DAY, and YEAR that you want the vacation message turned off.
7. Click **Set Deactivate Date**.
8. Click the **logout here** link at the top of the page.

Other Mailtools Filters

For all other Mailtools filters, on the Email Tools Web page, select the ACCC server that your email account is on, select **Set up Email Filters**, and click CONTINUE. After you login, you will be presented with the Email Filters Utility Page, which provides a number of different filtering options.

ANTISPAM Filter

The ready-made antispam filter can be activated to have spam automatically sorted out of your Inbox; see "Canned Spam Filters" on page 5 for more on this one.

ATTACHMENT Filter

There is also a ready-made filter for messages with attachments. Like the antispam filter, you can use it to sort email with attachments out of your Inbox or just to identify messages that have attachments. Turning the attachment filter on is just a matter of selecting whether you want to sort all attachments or just some (and selecting the ones you want from a list of extension types), and then selecting either **File matching messages into a folder:** or to tag them, **Tag only:**. (You can use the **Tag only:** action combined with a local filter to move selected messages into a local mailbox, which is explained in "Canned Spam Filters," on page 5.)

Sorting out all messages with attachments makes it much less likely that you'll open one accidentally, and it also makes them a lot easier to find. Even if you don't have much other mail, a large attachment or two can make you go over your email quota.

And we might develop more of these ready-made filters as the need arises.

Also, there's help to be had from a link on this page; click the **Help page in a new window** link at the top of the Email Filters Utility Page before you start working with your Mailtools filters.

CUSTOMIZABLE Filters

The most versatile of the Mailtools filters are the CUSTOMIZABLE filters. You can use these filters to automatically file messages into mailboxes (on the server only, remember, for use with WebMail, **pine**, or a personal computer email program set up to use IMAP), forward mail to other locations, or delete messages based on the criteria you specify. You'll naturally want to exercise some caution before choosing to delete a message though — if you accidentally make the criteria of a delete filter too broad, you could lose email that you really wanted to see. It's better to simply sort it into another mailbox and delete it by hand occasionally, once you're sure it's all junk.

For each filter you must specify two things.

The criteria used to select a message, based on whom it's from, whom it's addressed to, or what's in its subject line.

The action that should be done to the messages that match the criteria.

When selecting the action, first you choose one of:

- File the message into a folder (the Mailtools utility calls mailboxes folders), either an existing one or a new one created for the filter, or
- Forward the message to other email address(es), or
- Delete the message.

And then, as a separate choice, you choose whether to pass a copy of the message onto the filters that follow it and perhaps, eventually, into your Inbox. Select this, for example, if you want to forward the message to another address *and* to keep a copy for yourself.

Who Can Use Mailtools Email Filters?

Everyone, including you, can benefit from using Mailtools email filters. But how you can use them depends on how you read your email.

Regardless of how you read your email, if you're fed up with spam, try the Mailtools antispam filter, "Canned Spam Filters," page 5.

Regardless of how you read your email, when you're going on vacation and want to send automatic responses to the email messages that you receive while you're gone, use Mailtools. It's the right way to do it. And it'll keep you from embarrassing yourself by sending sixteen automatic replies to the same person or by sending auto replies to email discussion groups.

You might also want to throw in a few Mailtools customizable filters that will delete messages from email discussion groups while you're away; this could save your email account from going over your quota. If you receive a lot of email that you can't turn off, send an email message to **systems@uic.edu** asking that the email Grim Reaper be turned off while you're gone. Be sure to include your netid, email server, the day you're going, and the day you're coming back.

If you use Eudora (or Outlook or Netscape) with IMAP to manage your email, you've got the best of both worlds. Use Mailtools filters for email forwarding and deletion, vacation replies, and to sort out spam and attachments that you don't want to download automatically. Use Eudora filters for everything else, including moving incoming and outgoing messages to specific mailboxes, mainly because they're easier to set up. Ditto if you use IMAP with other personal computer email programs such as Outlook and Netscape.

If you use Eudora (or Outlook or Netscape) with POP to manage your mail, then, except for email forwarding or deleting, vacation notification, and the antispam and attachment filters, you're pretty much stuck with using only Eudora filters. Not that Eudora filters are bad, but you will always have to download all of your new incoming email, even mail that has attachments and mail that the antispam filter has identified as spam. Perhaps it's time to switch to IMAP?

If you always use WebMail or **pine**, then use Mailtools for all your filters. Neither WebMail nor **pine** have provisions to make their own filters.

The Tale of Ima Historian

The venturesome story of Ima Historian may help illustrate the usefulness of Mailtools customizable filters. Ima was subscribed to the email discussion list **roman_history@example.com**. But as you can imagine, the great interest in the list meant that there were simply too many messages coming in each day, which made it difficult and time consuming for Ima to sort through it to find her personal and more urgent messages.

So Ima decided to create a Mailtools filter to sort the mail from the list into her **Rome** mailbox, for leisure reading at home each night. For this she went to the Email Tools page, selected her email server machine and **Set up Filters**, clicked **CONTINUE**, and logged in to reach the Email Filters Utility Page.

On that page, she clicked **Create a new CUSTOMIZABLE mail filter**. Then, in the **Set criterion 1** box, she changed the options to read as follows: Activate filter if the **FROM:** field of the incoming email **contains** this: **roman_history@example.com**

She skipped the second criteria and jumped down to the **Set Action** section and selected **File this message into a folder:**. Since she had not yet created an **Rome** folder, she selected **create and use new folder:** and typed **Rome** in the box beside it. Because that was all she wanted done with these messages, she did not select the option to pass them on to the filters that follow it. After clicking **Create new Email filter**, all her new mail from the list was sorted into her **Rome** folder, and she was able to enjoy discussions on the conquests of Gaul in peace.

But the euphoria wore off quickly. Ima was also involved in a vehement email discussion on the use of Latin verbs in the Roman Senate, which was taking place on that same roman_history list. But this particular topic, being her specialty, was of much greater interest to her, so she needed to sort it out for more immediate attention.

So Ima created a second filter. This time she filled out the **Set criterion 1** options just as before, but then she combined it with a second criterion. In the section called **How should criterion 1 and criterion 2 be combined?**, she selected **AND**. Then, in **Set criterion 2**, she changed the options so that it read as follows: Activate filter if the **SUBJECT:** field of the incoming mail **contains** this: LATIN VERBS

Then, in the **Set Action** section, she choose to file these messages into a new folder called **verbage** just has she had done with **Rome** before.

But that evening, Ima was disappointed. In addition to her train home being late, she noticed that all of her mail from the roman_history list continued to be sorted into her **Rome** folder, regardless of whether the subject line contained "Latin verbs." But both of her filters were set up correctly — what had gone wrong?

Well, Rome wasn't built in a day. One thing to remember when creating email filters is that they are applied in the order that they're listed. In this case, as Ima's mail was received, each message was first compared to her first rule, and any mail from the roman_history list was put in her **Rome** mailbox.

Thus, *all* the mail from the roman_history list was sorted by the first rule and never made it to the second rule at all. Since her second rule was more specific than her first rule, it would have worked as planned had she created the second rule first.

Having realized this, Ima went back to the Web page to fix her error. She scrolled down to the section called **View, delete, or shuffle existing filters**, where the two filters she had made before were listed in the order she created them. In the box for the second filter, she clicked the button **Shuffle this filter up one position**. That changed the order of the two filters so Ima was now happy.

1. If mail was from roman_history AND about "Latin verbs," it went into her **verbage** folder.
2. If any remaining mail was from the roman_history list, it went into her **Rome** folder.
3. All remaining messages were filed in her Inbox.

Ima Historian is simply one example of a happy customer. If, like Ima, you receive an abundance of email and you're tired of sorting through it all for the important messages, then you could certainly put these filters to good use. But, while Ima's case was typical, there is much more you can do with the Mailtools email filters, which is explained on the page itself or its help page. Give it a try! You know the old saying, when in Rome...

Comments are welcome; please send them to Joshua Frigerio, **joshua@uic.edu**

About roman_history@example.com

Ima's roman_history list is made-up, but there is an ancient Mediterranean history email list, **ANCIEN-L@listserv.louisville.edu** and a number of related newsgroups:

http://groups.google.com/groups?hl=en&lr=&safe=off&group=soc.history

Illustration © 1996 Softkey International Inc. and its licensors.

Canned Spam Filters

Tech Tips

Any

Are you interested in an "Incredible Satellite TV offer?" Would you like to "Consolidate your debts in an offshore Visa card?" No? Well then, certainly you'd like to "Dig up Dirt on your Coworkers!" Still not interested? Then read on; you may be interested in the ACCC's new automatic spam filtering system.

You've probably seen phrases like those above in email messages you received but didn't request, that is, spam. We discussed the spam problem in the October/November/December 2000 issue of the *A3C Connection* in the article called "Slamming Spamming." That article covered the basics, what spam is, how it works, and some possible options to minimize the amount of spam you receive.

One such option is to filter out spam automatically. But a problem with automatic antispam filtering is that such filters can be very complicated to set up, and they can dispose of valid email if not crafted carefully. We have tried to remedy this by providing an automatic and simple way to set up effective antispam email filters, i.e., Canned Spam Filters.

While the Mailtools antispam filter will probably catch most of the spam mail you receive, it won't catch all of it — a perfect antispam filter is impossible. Some spam will inevitably slip by, so you can't forget where your **Delete** key is yet, but hopefully your clicking finger will get much less work with this filter in place.

Likewise, although we have taken care to make this unlikely, it is also possible that a valid piece of email will somehow be sorted in with the spam, so you should check through your filtered spam messages from time to time to make sure you didn't miss anything that you wanted to see — the notification of your lottery winnings, for example.

Setting Up Your Antispam Filter

To set up your own antispam filters, visit our Email Tools Web utility at **http://www.uic.edu/htbin/accc/mailtools** and select the option **Set up Email Filters**. Once you've logged in, select **Create a new ANTISPAM filter**.

Setting up the antispam filter is done in three steps. The first two steps must be done accurately to avoid legitimate email from being filtered out as spam.

Step 1: Enter any email addresses that you use other than to your normal UIC email address (or addresses — your netid at host name that ends with **uic.edu**). For example, you may have an account such as **imah@example.com**, which simply forwards mail from there to your UIC account. In this case, enter **imah@example.com** into the box in Step 1, it will prevent messages addressed to you there as being counted as spam.

Additionally, you may have a departmental alias at UIC that simply forwards mail to you. If you get mail sent to **latinverbs@uic.edu**, for example, then entering that address here will tell the filter that it is valid email and should not be sorted as spam.

Step 2: To prevent messages from email discussion lists from being counted as spam, type the email address of all lists to which you are subscribed in the box, not including any here at UIC — UIC lists are automatically excluded from the filter. For instance, do you subscribe to **bubblegumweekly@stickylists.com**? Then you'll need to put that address into the box in Step 2.

Of course, if you forget to identify any of your alternate email addresses or email discussion lists, the filter will identify messages to them as spam, so you'll want to be sure to check your spam folder frequently at first to see if any messages got through from lists you forgot to include. You can imagine that, if you subscribe to many lists, it may take a few tries before you get it quite right.

*Step 3: If you use WebMail, **pine**, or Eudora or another personal computer email program with IMAP, you'll probably want to choose the action* **File this message into my spam folder**. Thus, once an email message is identified as being spam, it will automatically be sorted into another folder on the server called **spam**, which you should check at your leisure and delete the messages that are really spam.

That's it! Just click the **Create Antispam filter** button below Step 3 to begin your no-spam diet.

If you'd like to know how the antispam filter works, see "How the Mailtools Filters Work" on page 6.

What If You Use Eudora, etc., with POP?

You can still use the Mailtools ready-made antispam (and attachment) filter, using the other action option, **Tag only:**. This action adds a hidden tag to each spam email message. (What they actually add is an X-header; see the online version of "Figure 2: Headers of a Legit Email Message," from the October/November/December 2000 *A3C Connection*, **http://www.uic.edu/depts/accc/newsletter/adn29/legitmail.html**)

You then use this hidden tag as a criterion in a Eudora local filter so that Eudora will recognize the email message as spam and move it into a local spam mailbox on your personal computer. Figure 1 below is a Eudora filter that will do that.

Oops, Did You Forget Something?

Did you forget to add an email discussion list? An off-campus address? No problem. Just return to Email Filters page and jump down to the section where you created the antispam filter. There you'll see that the alternate addresses and off-campus lists that you entered before appear in the boxes where you typed them. Simply edit the lists and click the button again and your changes will take effect immediately.

Comments are welcome; please send them to Joshua Frigerio, **joshua@uic.edu**

How Mailtools Filters Work

Tech Tips Any Expert

In General

When mail arrives on the server that is destined for your account, it is handed off to a program called procmail. Before procmail delivers a message into your Inbox, it looks to see if you have a file in your home directory called **.procmailrc**, and, if you do, it looks inside for instructions on how to deliver the message.

The Mailtools Web interface for creating email filters translates the criteria and action you specify into procmail "rules" and places the rules in your **.procmailrc** file. Sounds simple, and it is, but the problem is that the procmail language is incredibly complicated. Consider, for example, Ima Historian's filter for mail from the roman_history list that contain "latin verbs" in the subject. Here is the procmail rule that Mailtools created for Ima:

```
:0 :
 * ^FROM:.*roman_history\@example\.com
 * ^Subject:.*LATIN\ VERBS
 mail/verbage
```

Not only is the text cryptic, but each colon and slash and asterisk and caret mean something specific, and the placement of the commands on the lines is also significant. Creating a set of functional procmail filters by hand is not for the faint of heart.

You can read more about procmail by logging into your tigger or icarus account and looking at the man pages for **procmailex** (examples), **procmailrc** (about the procmailrc file), and **procmail**, in that order. (Enter: **man procmailex** and so on.) If you do, you will see that the Mailtools filters use only a small fraction of the services that procmail provides. If you want to venture further into procmail, a good way to start is to create some filters with the Web interface and then edit the **.procmailrc** file it creates for you as you desire. Note, however, that the Web interface tools will not work anymore on any filters you change manually.

If you already have a **.procmailrc** file, and you will know if you do, you can use the Mailtools interface

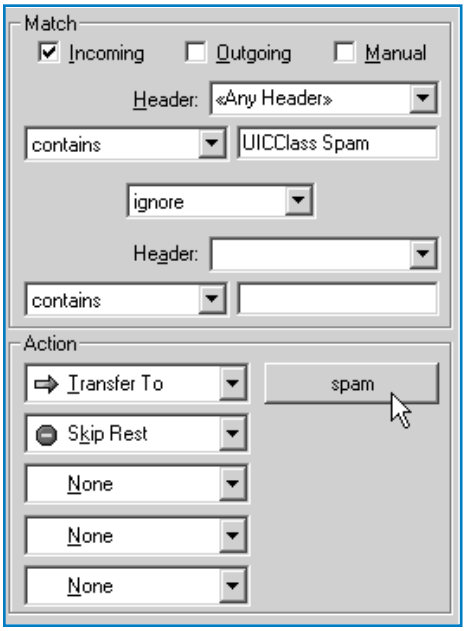

Figure 1: Eudora Filter For Mailtools Tag only: Action

This filter selects email with the Mailtools antispam filter's **X-UICClass: UICClass Spam** header and moves them to a separate local mailbox named **spam**. An equivalent filter for the Mailtools ready-made attachment filter would be **<<Any Header>> contains UICClass Attachment**. This should be your last Eudora filter. For more info, see "How to Make a Eudora Filter" at: **http://www.accc.uic.edu/software/eudora/eudora.win.html#filter**

to create additional filters; the Mailtools filters will be added to the bottom of your existing **.procmailrc** file and therefore will be applied last. If you want them to be applied somewhere else, you'll have to move them by hand. But be sure not to change the text of the Mailtools filters if you do.

The Antispam Filter in Particular

The Mailtools antispam rule set is rather long and complicated, and it may be changed as circumstances change. So, instead of placing the entire rule into your **.procmailrc** file, the Mailtools utility places a line into your **.procmailrc** file that tells procmail to include the global antispam filter in your rules at that point. The global antispam filter is located in a global directory with some other ready-made filters.

The procmail rules finally chosen to compose the antispam filter were selected from a large set of possible methods for determining whether a piece of incoming mail is indeed spam. The rules now in use for this filter were chosen after careful research was done on the efficacy and efficiency of each. Thus, they may also change in the future: new spamming techniques may render certain methods more or less applicable, or new hardware may allow us to use less efficient filters.

The first and most effective method employed in the Mailtools antispam filter is simply to take advantage of the laziness of most spammers. Currently, eighty to ninety percent of spam mail is sent without a valid **To:** or a valid **Cc:** header. That is, these fields, if they are present at all, do not contain your email address. They simply use the same set of headers for every piece of mail sent. Mail sent from colleagues or friends, however, will almost never look like this. (Unless it's "bounced" to you or sent as a blind carbon copy, **Bcc:**. That's another reason why you shouldn't immediately delete all spam and why you should check your spam mailbox on a regular basis.)

Email discussion lists like Ima's roman_history list are an exception to this rule: they usually distribute mail without your address in the **To:** or **Cc:** field. Thus the only way to determine whether any piece mail is valid is for you to specify the lists to which you are subscribed.

So, the first set of rules in the antispam filter mark any mail as spam that is a) not addressed to you or b) not from a valid list or address as defined by you. Using these criteria will catch a large fraction of the spam you receive.

Unfortunately, the efficacy for identifying the rest of your spam decreases dramatically at this point. Of the ten percent or so of spam that makes it through the first step undetected, you might expect an additional ten percent or so of the remaining spam (i.e., two percent) to be caught by the next set of rules, which we call "headercheck" rules.

The headercheck rules check through the headers of each email message for common signs that the mail is spam. For example, if the mail contains invalid header tags, empty or missing **To:** fields, empty or missing **From:** fields, missing or invalid message ids, invalid **From:** settings, invalid IP addresses, header forgeries, and so on.

As of now, these two are the only rule sets in the Mailtools antispam filters. There are many additional methods for identifying spam in use elsewhere, which we tested for inclusion in our antispam filters. Our tests showed them all to be either ineffective, too dynamic (requiring constant maintenance or updates), or too inefficient (requiring too much CPU time for the amount of mail we receive).

For example, there are organizations that try to keep track of spammers and the hosts from which they send their spam, and they make these lists publicly available. Such organizations include the Realtime Blackhole List, Spamhaus, and so on. The theory is that you check the hostname of the machine that each new message originally came from against a list of known spamming hosts. If a host is on a list of spammers, then any message from it is spam.

Our tests, however, showed that not even one percent of spam messages were identified by this kind of rule. And these lists sometimes include, accidentally or otherwise, hosts from which there are innocent senders. Additionally, this rule would also require constantly connecting to these other sites to check the hostnames, or constantly updating and maintaining local lists received from these sites.

In summary, the two sets of filters mentioned above comprise the antispam methods we've decided to offer via the Web interface. They are a first attempt at mixing accuracy, effectiveness, and simplicity into taking a palatable bite out of spam.

Comments are welcome; please send them to Joshua Frigerio, **joshua@uic.edu**

SSH: Do You Know Where Your Password Is?

News on the Net

You've listened when we told you to be careful with your password, haven't you? You never write it down, you don't tell it to your friends, you don't save it in Eudora, and you don't enter it on the Web except when you use WebMail or when you're asked for it by the UIC WWW Identification Service, a.k.a. Bluestem. When you choose your passwords you don't use your spouse's name or your dog's name and you don't use a dictionary word that could be guessed.

That means your password is safe, doesn't it?

Well, not really. Each time you login to your borg, icarus, or tigger account, after you type your password and press **Enter**, your password is sent out over "the network." That ******* stuff you see as you type your password is just to fool anyone who's looking over your shoulder — your actual password is sent over the network "in the clear," exactly as you typed it. That means that it could be intercepted and read by anyone else who's on the same network.

Privacy and Logging In

When last we visited the idea of privacy and security on the Internet ("Pretty Good Personal Privacy," January/February/March 2000), we talked about using encryption to keep email messages and files secure. The same considerations apply to remote logins — you have every right to expect security for your interactions when you're logged in to a remote host machine:

Authenticity: Being able to tell without a doubt what the source of the data is. Your password tells the server who you are, but that's only half of the question; the server should also assure you who it is.

Privacy: Scrambling data so it can't be used by anyone except the person that it's intended for. Privacy in remote logins means encrypting your password and, for that matter, your entire login session, so only you and the server you log into can read it.

Integrity: Assurance that the server is receiving everything you send it, nothing more, nothing less. And vice versa — assurance that you're receiving the exact messages, output, and files the server sends you, nothing more, nothing less.

Yes, remote logins are vulnerable in all these areas. Say you're going from *here* to *there*. If the route from here to there goes though someone else's network, a bad guy on that network could eavesdrop on your transmission, looking for passwords, credit card numbers, or business secrets. Or they could use IP spoofing to redirect your communications to a fake server.

What's Safe besides SSH? Bluestem, WebMail, ACCC Dialins (sort of)

Bluestem logins and all of WebMail are safe; they use SSL (Secure Sockets Layer), the secure Web protocol that encrypts all Web traffic to and from the server. You can tell they're secure because your browser's lock icon will be locked and because their URLs begin with **https://**, rather than **http://**. We talked about SSL and Bluestem in the March/April 1997 *A3C Connection:* **http://www.accc.uic.edu/newsletter/adn16/**

Security and convenience is why you probably should read your email with WebMail when you're traveling. To be completely safe when you use WebMail on a borrowed personal computer, you probably should delete the browser's "temporary Internet files" when you're done.

In Internet Explorer: **Tools→Internet Options…**, click **Delete Files…**, then click **OK** (don't select **Delete all offline content** on a borrowed machine).

In Netscape: **Edit→Preferences→ Advanced→Cache**, then click **Clear Memory Cache** and **Clear Disk Cache**.

Logging into the ACCC dialin lines is also safe — someone would have to be bugging your phone to intercept your password then.

Traffic over the ACCC dialin lines to the ACCC email/UNIX servers is also reasonably secure; someone would have to have broken into one of the important ACCC machines to do any damage there. (Keeping our public machines secure is a major and continuous commitment of the ACCC.) Traffic on campus from a switched LAN to the major ACCC machines is also probably not sniffable, although that comes with less of a guarantee.

But if you come into UIC from outside on the Internet, either from a commercial ISP or from another organization's network, *or if you go out to the Internet from the UIC network,* then you're no longer safe. Login to a remote host system, and there goes your password out over a public computer network, probably in the clear. Your password and connection will be vulnerable in each network that it goes through.

Or the bad guy on a machine that's somewhere in the middle of your route from here to there could intercept your traffic and respond to you as if it was there and respond to there as if it was you. That's called a "man-in-the-middle" attack, and if the man in the middle is careful, you wouldn't even know it happened to you.

SSH: Strong Security for Remote Logins

But you don't have to worry about any of that. Transparent security for logins is here — secure remote logins with secure shell or SSH. SSH provides a secure replacement for telnet (with a secure and easy way to do X Windows; see "Secure X Windows with SSH", page 10); for the UNIX "r" commands, **rsh**, **rlogin**, and **rcp**; and for FTP.

SSH's security is transparent because it's an application layer protocol — you use SSH software to login to a remote host instead of using telnet. And SSH really is secure. It supplies two-way authentication, including the server authenticating itself to you. After exchanging keys, your entire login session is encrypted, including your password and everything that you send to the host server and everything it sends to you.

The best thing about SSH is that all this security stuff goes on behind the scenes. From your point of view as a user, an SSH application looks like just another version of telnet.

It's no harder to switch to an SSH secure remote login application than it is to change from one vendor's telnet to another's.

Interested? We're going to include SSH Secure Shell for Windows in the new NSKit. But you don't have to go out and get the whole kit to get SSH. You can download SSH Secure Shell for Windows from the **ftp.uic.edu** FTP server. (See figure 2 and its caption.) Version 2.3 is on the FTP server as I write this, but it's possible that Version 2.4 will be available by the time this article is published. The information in this article and in the ACCC Web page on SSH Secure Shell, **http://www.accc.uic.edu/software/ssh/**, applies to both versions.

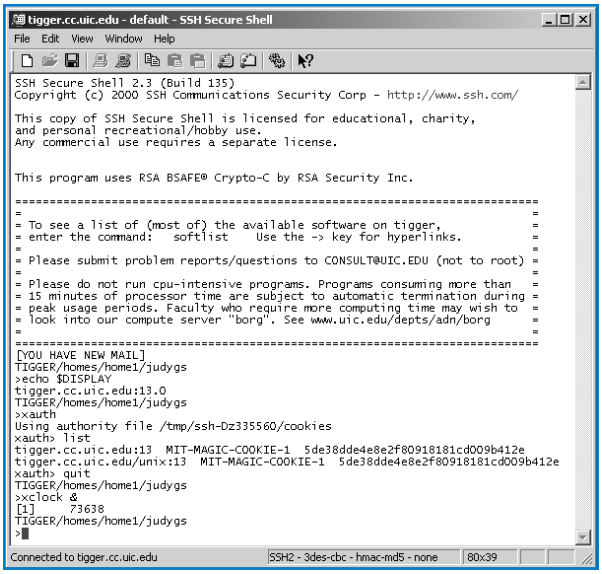
tigger.cc.uic.edu - default - SSH Secure Shell
File Edit View Window Help
SSH Secure Shell 2.3 (Build 135)
Copyright (c) 2000 SSH Communications Security Corp - http://www.ssh.com/
This copy of SSH Secure Shell is licensed for educational, charity,
and personal recreational/hobby use.
Any commercial use requires a separate license.
This program uses RSA BSAFE® Crypto-C by RSA Security Inc.
To see a list of (most of) the available software on tigger,
enter the command: softlist Use the -> key for hyperlinks.
Please submit problem reports/questions to CONSULT@UIC.EDU (not to root)
Please do not run cpu-intensive programs. Programs consuming more than
15 minutes of processor time are subject to automatic termination during
peak usage periods. Faculty who require more computing time may wish to
look into our compute server "borg". See www.uic.edu/depts/adn/borg
[YOU HAVE NEW MAIL]
TIGGER/homes/home1/judygs
>echo $DISPLAY
tigger.cc.uic.edu:13.0
TIGGER/homes/home1/judygs
>xauth
Using authority file /tmp/ssh-Dz335560/cookies
xauth> list
tigger.cc.uic.edu:13 MIT-MAGIC-COOKIE-1 5de38dde4e8e2f80918181cd009b412e
tigger.cc.uic.edu/unix:13 MIT-MAGIC-COOKIE-1 5de38dde4e8e2f80918181cd009b412e
xauth> quit
TIGGER/homes/home1/judygs
>xclock &
[1] 73638
TIGGER/homes/home1/judygs
Connected to tigger.cc.uic.edu
SSH2 - 3des-cbc - hmac-md5 - none
80x39

Figure 2: Logging in with SSH Secure Shell

Download a self-extracting archive of SSH Secure Shell from the ftp.uic.edu FTP server: **ftp://ftp.uic.edu/pub/othersoftware/ssh/**
The $DISPLAY variable and the xauth list command output in the window shows how SSH X11 tunneling works with X Windows; see "Secure X Windows with SSH," page 10.

Confused by the Names?

SSH Secure Shell, the software, was written in 1995 by Tatu Ylönen, a Finish computer scientist. Both "SSH" and "secure shell" are trademarks of his company, SSH Communications Security Corp. The U of I has a site license for their products.

The SSH code, however, is freely available and is used in a number of other secure remote login applications, for a wide range of operating systems; see: **http://linuxmafia.com/pub/linux/security/ssh-clients** for an up-to-date list and links.

SSH the protocol (which SSH Communications would prefer that we call SECSH) has not been approved as an IETF standard yet, but they're working on it; the protocol drafts are maintained by SSH Communications:
http://www.ssh.com/tech/archive/secsh.html
The SSH FAQ should answer any other questions you might have about SSH:
http://www.employees.org/~satch/ssh/faq/

To Install SSH Secure Shell

1. Download **sshwin-2.3.0.exe** from **ftp://ftp.uic.edu/pub/othersoftware/ssh/**
2. Double-click on the file's icon to unpack and install SSH Secure Shell. The EXE file will install the program in your **C:\Program Files\SSH Communications Security** directory; the NSKit will install it in your **C:\Program Files\UICNSkit\SSH** directory.
3. If you're going to use SSH with X Windows, turn on X11 Tunneling before you connect. (Saving the settings when you close SSH will keep them to apply to future sessions.)
   a. Open SSH (see below), then click **Edit→Settings…**
   b. Click **Tunneling** under **Host Settings**; click in the box next to **Tunnel X11 Connections**, and then click **OK**.
   c. Close SSH. It'll ask you whether you want to save the changes you've made; click **Yes**.

For More Info

I think you'll find that SSH Secure Shell works a lot like whatever telnet you've been using, but don't stop there; it can do lots more.

The SSH Secure Shell user manual is in its online help and is on the Web at: **http://www.ssh.com/products/ssh/winhelp/**
Or see the ACCC document: **http://www.accc.uic.edu/software/ssh/**

To Login Using SSH Secure Shell

1. Open SSH using either: **Start→Programs→SSH Security→SSH Secure Shell**
   or: **Start→Programs→Network Services Kit→Secure Shell→SSH Secure Shell**
2. Press **Enter**.
3. In the **Connect to Remote Host** dialog box, type the host name and your login ID in the **Host Name:** and **User Name:** fields; say, for example, *tigger.cc.uic.edu* and your ACCC netid. Press **Enter** or click **Connect**.
4. If this is the first time you've used SSH Secure Shell to connect to this remote host, SSH will show you the host's public key and ask you: "Do you want to save the new host key to the local database?" If you trust this is the right host, click **Yes** to save it. (Trust is involved, as it has to be.)
5. The **Enter Password** dialog box opens. Type your password in the **Password:** box, and press **Enter** or click **OK**.

Using SSH Secure sFTP

Login with SSH to the host you want to exchange files with, then select **Window→New File Transfer** or click the file transfer icon, a file folder with a quarter circle of blue dots over it. The **Secure File Transfer** window works like Windows Explorer for the files on the remote host, with the directory tree of your account on the left and the directories and files in current the directory on the right.

To download, select a file to download and click the download icon ⇩. To upload, open the directory you want upload a file into and click ⇧. Or drag and drop files, up or down, as you would in Explorer. To change a file's UNIX access permissions, right-click on a UNIX filename and select **Properties**. (SSH File transfer calls them "Attributes".)

To Exit SSH Secure Shell

Logoff from your UNIX account, then either select **File→Exit** or click the Close box in the upper right corner of the SSH Secure Shell window.

Secure X Windows with SSH

News on the Net **UNIX Expert**

The X Windows system is a GUI — graphical user interface — that allows you to display the graphical output from commands that are run on a remote UNIX system on your local system — in this case, your personal computer. This allows your personal computer to do what it does best — display output — while the remote UNIX system does what it does best — running programs or number crunching.

There are two classes of UNIX programs that benefit from using a X Windows display: number crunching programs that produce graphical output, such as SAS, SPSS, Octave (MATLAB clone), and Maple; and utility programs such as **ghostview** (PostScript document viewer), **xrn** (newsreader), **info** (online IBM manuals on tigger), and **xbsub** et al. (programs to manage jobs run on borg).

If you already use X Windows on an MS Windows personal computer at UIC, then chances are you're using Hummingbird Communications' Exceed X Server. Exceed is part of the Hummingbird Communications package, which includes various communications tools and the UNIX **tar** compression and archiving tool.

Exceed is available at UIC on the Windows personal computers in the ACCC public labs, via ACCC Server Services, and may be purchased under a site license by UIC faculty and staff. (Go to the ACCC home page, **http://www.accc.uic.edu/**, click the **Software** button, and select **Public Labs - Software**, **Server Services**, or **Site-Licensed Software**.)

As is usual for anything UNIX, there are several different ways you can set up and use an X Server. The two easiest ways are:

Using insecure Xhost security, where permissions are given based on the remote host's name, allowing anyone logged on to that remote host to open an X Window on your personal computer or worse (see "Xhost 'Security'" on page 11).

Using secure SSH X11 tunneling, which limits access to your X server only to X Windows programs that you start and which is much easier to set up, too.

So the question is: insecure and harder vs. secure and easier. SSH X11 tunneling wins hands down.

How X Windows Works with SSH

X Windows is client/server software, where the "client software" request services from a "server". Normally, you run the client software on your personal computer and the server is on a remote computer. But in X Windows, client/server software works the other way around. You run an X Server, such as Exceed, on your local machine, and client processes running on a remote UNIX machine use your X Server to display their output on your local machine.

While this local server/remote client idea makes sense for X Windows, it vastly complicates the client/server security question — how to determine which client processes on which remote machines should be allowed to display their output using the X Server on your personal computer.

The obvious answer is only those client processes that you start using your own UNIX account(s). Unfortunately, that is hard to do. So people often set their X Servers up by defining "trusted hosts" using Xhost security. Xhost security gives any account on a specific UNIX host permission to open an X Windows window on your personal computer and much worse (see the box).

SSH with X11 tunneling, on the other hand, is both easy to set up and secure because it puts the client software back on your personal computer. You can use it on your personal computer with your local X Server to run X Windows from any remote UNIX host that you have an account on and that supports SSH X11 tunneling, without changing any settings on your X Server or on the remote host.

When using SSH's X11 tunneling, you set your X Server up with Xhost security, but you tell it that the only host it should trust is the **localhost** — your own personal computer. Then you use SSH in place of telnet to login to your account on the remote host. As part of the login process, your SSH client software negotiates with the SSH server on the remote host, and together, they automatically set up a secure X-Windows connection between your account on the remote host and your X Server (figure 2, page 9).

Xhost "Security"

The "access to your X server" that Xhost security gives to other accounts on the remote host is much worse than just being able to open X Windows windows on your monitor. It means that a bad guy can *read* all the windows managed by your X Server, including those where you typed passwords, regardless of whether you can read the password on your screen. And it means being able to change X Server settings that are read by other clients.

This really should scare you.

Does Your UNIX Host Support SSH X11 Tunneling?

The ACCC public UNIX servers do. If your favorite UNIX host doesn't support SSH X11 tunneling yet, ask its administrators to install it. Use an OpenSSH server, **http://www.openssh.com/**, or the SSH Communications servers on the UIC FTP site (figure 2, page 9).

Setting Up to Use X11 Tunneling

You only have to do this once; that's a good thing.

1. Set up Exceed for X11 tunneling.

Install and configure Exceed for Passive Communications and Multiple Windows, following the instructions in "Using Exceed X Server with SSH X11 Tunneling," **http://www.accc.uic.edu/software/exceed/sshexceed.html**.

When you use SSH X11 tunneling, the only host that Exceed talks to is your own personal computer. So you set Exceed up to use Xhost security, but, regardless of which or how many UNIX machines you're going to use X Windows with, you tell Exceed to answer to only one machine — your local host, a.k.a **localhost**. "Using Exceed X Server with SSH X11 Tunneling" explains how to do this.

If your **xhost.txt** file already has other specific UNIX hosts listed, such as icarus, tigger, or an EECS machine, *delete those lines*.

2. Set up your host account, if necessary.

If you've never used your UNIX account with X Windows, then you're set. You don't have to do anything more than just login using SSH. Ever.

If you have used your UNIX account with X Windows before, then you've probably set it up to talk to your X Server. If so, you have to remove those settings. The "Using Exceed X Server with SSH X11 Tunneling" Web page explains how.

Running X Windows with SSH

1. Start your X Server: **Start→Programs→Hummingbird→Exceed→Exceed** (Do not select **Exceed (XDMCP-Broadcast)**.)
2. Start SSH X11 tunneling: Log in to your UNIX account with SSH set up with X11 tunneling turned on (page 9).
3. Run an X Windows program on UNIX: **x clock** is good to use for testing. Enter: **xclock &** and an X Windows window containing a clock will open. It might open minimized; if you don't see it right away, check your taskbar.

And that's all there is to it.

Comments are welcome; please send them to Judith Grobe Sachs, **judygs@uic.edu**

UIC University of Illinois at Chicago

The A3C Connection
Academic Computing and Communications Center (MC 135)
Room 124 Benjamin Goldberg Research Center
1940 West Taylor Street
Chicago, Illinois 60612-7352

About The A3C Connection

The A3C Connection is published four times per year by the UIC Academic Computing and Communications Center, providing news and information about the use of computers, communications, and networking at UIC. It is edited by Judith Grobe Sachs with help from Bill Mayer and the UIC Office of Publications Services.

Distribution of the *A3C Connection* is free to UIC faculty, staff, and students, and to other universities and not-for-profit organizations. To subscribe, send us your name and address, UIC campus address if possible, including your department name and mail code. To cancel your subscription, send us your address label or a copy of all the information on it.

Contact us by electronic mail at **connect@uic.edu**; by telephone at the Client Service Office, (312) 413-0003; by US Mail at The A3C Connection, ACCC (MC 135), Room 124 Benjamin Goldberg Research Center, University of Illinois at Chicago, 1940 West Taylor Street, Chicago, Illinois 60612-7352; or by fax at (312) 996-6834.

We welcome any comments, suggestions, complaints, or requests you might have concerning the *A3C Connection*.

The Fine Print

The use of trade, firm, or corporation names in this publication is for the information and convenience of the reader. Such use does not constitute an official endorsement or approval by the University of Illinois of any product or service to the exclusion of others that may be suitable. Trade names that may appear in this publication include the following: Apple, the Apple logo, Mac, Mac logo, and Macintosh (registered trademarks of Apple Computer, Inc.); AIX and AIX/ESA (registered trademarks of IBM Corp.); UNIX (registered trademark of The Open Group); HP and HP-UX (registered trademarks of Hewlett-Packard Corporation); Sun, Solaris, and Java (registered trademarks of Sun Microsystems, Inc.); and Microsoft, Windows, Windows NT, and other Microsoft product names (trademarks or registered trademarks of Microsoft Corporation). All other product names mentioned herein are used for identification purposes only, and may be the trademarks or registered trademarks of their respective companies.

Permission is granted to reprint or adapt all or part of the *A3C Connection* for nonprofit use, provided that full acknowledgment of the source is given.